

Docket No. 200314912-1
Application No.: 10/827,218

RECEIVED
CENTRAL FAX CENTER
OCT 20 2008

Amendments to the Claims:

Status of Claims:

- Claims 1-18 and 45-46 are pending for examination.
Claims 19-44 and 47 were withdrawn by the examiner.
Claims 19-44 and 47 are canceled herein as non-elected claims.
Claims 48 and 49 are added herein.
Claims 1, 5, and 45 are in independent form.

1. (Currently Amended) A system, comprising:

a logic configured to perform ~~one or more of~~, cryptographic key maintenance, ~~and cryptographic key migration~~ for a trusted platform to which the logic ~~may be~~ is bound in a one-to-one manner, where the cryptographic key maintenance includes migrating a non-migratable storage root key from a root of a key storage hierarchy associated with a trusted platform module associated with the trusted platform; and

an interface configured to facilitate operably connecting the system to the trusted platform.

2. (Currently Amended) The system of claim 1, where the cryptographic key maintenance ~~and the cryptographic key migration~~ performed by the logic comply with the Trusted Computing Group (TCG) specification version 1.1b.

3. (Original) The system of claim 1, where the logic comprises an application specific integrated circuit (ASIC).

4. (Original) The system of claim 1, where the logic comprises a microprocessor operably connected to a non-volatile memory.

5. (Currently Amended) A ~~[[The]]~~ system of claim 1, comprising:

Docket No. 200314912-1
Application No.: 10/827,218

a logic configured to perform one or more of, cryptographic key maintenance, and cryptographic key migration for a trusted platform to which the logic is bound in a one-to-one manner; and

an interface configured to facilitate operably connecting the system to the trusted platform;

where the logic and the interface comprise part of a USB token.

6. (Currently Amended) The system of claim 5 [[1]], where the logic is configured to migrate one or more non-migratable keys from a trusted platform module associated with the trusted platform and configured to use the migrated one or more non-migratable keys to decrypt items that were encrypted by the trusted platform module ~~where the interface is configured to facilitate operably connecting the system to the trusted platform by one or more of, a Universal Serial Bus interface, a Small Computer Systems Interface interface, a Peripheral Component Interconnect interface, a PCI Express (PCI-E) interface, a 1394 interface, an Industrial Standard Architecture interface, an Extended Industrial Standard Architecture interface, a wireless connection, and a microchannel interface.~~

7. (Currently Amended) The system of claim 1, where the logic is configured to perform ~~performing~~ cryptographic key maintenance ~~includes~~ including cloning the trusted platform with the cooperation of a manufacturer of the trusted platform and an owner of the trusted platform.

8. (Currently Amended) The system of claim 7, where the logic is configured to perform ~~performing~~ cryptographic key maintenance ~~includes~~ including having the manufacturer of the trusted platform act as an intermediary and migrating [[a]] the non-migratable storage root key from [[a]] the root of [[a]] the key storage hierarchy associated with [[a]] the trusted platform module associated with the trusted platform.

Docket No. 200314912-1
Application No.: 10/827,218

9. (Currently Amended) The system of claim 1, where the logic is configured to perform performing cryptographic key migration ~~includes~~ including logically attaching a trusted platform module migratable key data structure associated with a first protected storage tree to a second protected storage tree.

10. (Currently Amended) The system of claim 1, where the logic is configured to store one or more of, a copy of a storage root key, a binding data that facilitates binding the logic to the trusted platform in a one-to-one binding, a processor executable set of instructions that facilitate the trusted platform determining that the trusted platform is interfacing with the logic instead of ~~[[a]]~~ the trusted platform module, and a processor readable set of data that facilitates the trusted platform determining that the trusted platform is interfacing with the logic instead of a trusted platform module.

11. (Currently Amended) The system of claim 1, where the logic is configured to facilitate substantially instantaneously restoring ~~[[a]]~~ the trusted platform module.

12. (Currently Amended) The system of claim 1, where the logic is configured to decrypt one or more of, a key, and a piece of data encrypted by ~~[[a]]~~ the trusted platform module.

13. (Original) The system of claim 1, where the logic is configured to execute processor executable instructions associated with the logic while preventing execution of processor executable instructions not associated with the logic.

14. (Original) The system of claim 1, where the logic is configured to read processor readable data associated with the logic while preventing a second logic from reading the processor readable data associated with the logic.

15. (Original) The system of claim 1, where the logic is configured to detect whether there is a functional trusted platform module associated with the trusted platform.

Docket No. 200314912-1
Application No.: 10/827,218

16. (Original) The system of claim 1, where the logic is configured to prevent creation of a new cryptographic key by the system and to prevent performance of an attestation service by the logic.

17. (Original) The system of claim 1, where binding the logic to the trusted platform in a one-to-one manner includes producing an optimal asymmetric encryption padding (OEAP) binary large object to facilitate copying a storage root key stored in a trusted platform module associated with the trusted platform.

18. (Currently Amended) The system of claim 1, where the logic is configured to perform a finite number of cryptographic key maintenance or migration operations.

19. – 44. (Canceled)

45. (Currently Amended) A system, comprising:

an electronic apparatus configured with a trusted platform module; and
an interface operably connected to the electronic apparatus, the interface configured to facilitate operably, detachably connecting a subordinate trusted platform module to the electronic apparatus; and
a subordinate trusted platform module to communicate with the trusted platform module via the interface, the subordinate trusted platform module including logic to migrate a non-migratable storage root key from the trusted platform module to be stored within the subordinate trusted platform module.

46. (Original) The system of claim 45, where the electronic apparatus comprises one of, a computer, a printer, a cellular telephone, and a digital camera.

47. (Canceled)

Docket No. 200314912-1
Application No.: 10/827,218

48. (New) The system of claim 45 where the interface includes a port, and the subordinate trusted platform module is embodied in a removable component that is attachable and detachable to the port.

49. (New) The system of claim 45 where the subordinate trusted platform module is configured to use the migrated non-migratable storage root key to decrypt items that were encrypted by the trusted platform module.